

CHRISTOPHER COX, CALIFORNIA,
CHAIRMAN

JENNIFER DUNN, WASHINGTON,
VICE CHAIRMAN
C.W. BILL YOUNG, FLORIDA
DON YOUNG, ALASKA
F. JAMES SENSENBRENNER, JR., WISCONSIN
W.J. "BILLY" TAUZIN, LOUISIANA
DAVID DREIER, CALIFORNIA
DUNCAN HUNTER, CALIFORNIA
HAROLD ROGERS, KENTUCKY
SHERWOOD BOEHLERT, NEW YORK
LAMAR SMITH, TEXAS
CURT WELDON, PENNSYLVANIA
CHRISTOPHER SHAYS, CONNECTICUT
PORTER J. GOSS, FLORIDA
DAVE CAMP, MICHIGAN
LINCOLN DIAZ-BALART, FLORIDA
ROBERT W. GOODLATTE, VIRGINIA
ERNEST J. ISTOOK, JR., OKLAHOMA
PETER T. KING, NEW YORK
JOHN LINDER, GEORGIA
JOHN B. SHADEGG, ARIZONA
MARK SOUDER, INDIANA
MAC THORNBERRY, TEXAS
JIM GIBBONS, NEVADA
KAY GRANGER, TEXAS
PETE SESSIONS, TEXAS
JOHN E. SWEENEY, NEW YORK

JOHN GANNON
STAFF DIRECTOR

STEPHEN DEVINE
*DEPUTY STAFF DIRECTOR AND
GENERAL COUNSEL*

THOMAS DILENCE
*CHIEF COUNSEL AND
POLICY DIRECTOR*



One Hundred Eighth Congress
U.S. House of Representatives
Select Committee on Homeland Security
Washington, DC 20515

JIM TURNER, TEXAS,
RANKING MEMBER

BENNIE G. THOMPSON, MISSISSIPPI
LORETTA T. SANCHEZ, CALIFORNIA
EDWARD J. MARKEY, MASSACHUSETTS
NORMAN D. DICKS, WASHINGTON
BARNEY FRANK, MASSACHUSETTS
JANE HARMAN, CALIFORNIA
BENJAMIN L. CARDIN, MARYLAND
LOUISE M. SLAUGHTER, NEW YORK
PETER A. DEFazio, OREGON
NITA M. LOWEY, NEW JERSEY
ROBERT E. ANDREWS, NEW JERSEY
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ZOE LOFGREN, CALIFORNIA
KAREN MCCARTHY, MISSOURI
SHEILA JACKSON-LEE, TEXAS
BILL PASCRELL, JR., NEW JERSEY
DONNA M. CHRISTENSEN, U.S. VIRGIN ISLANDS
BOB EATHERIDGE, NORTH CAROLINA
KEN LUCAS, KENTUCKY
JAMES R. LANGEVIN, RHODE ISLAND
KENDRICK B. MECK, FLORIDA
BEN CHANDLER, KENTUCKY

DAVID SCHANZER
*DEMOCRATIC STAFF DIRECTOR AND
CHIEF COUNSEL*

MARK T. MAGEE
DEMOCRATIC DEPUTY STAFF DIRECTOR

August 3, 2004

The Honorable Tom Ridge
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Ridge:

The Homeland Security Act requires the Department of Homeland Security (DHS) to conduct a comprehensive vulnerability assessment of critical infrastructures and key assets in the United States, as well as to prioritize infrastructures for protection and assist relevant entities in protecting such infrastructures. A daunting task, the vulnerability assessment requires DHS to put in place a standardized and easily-understood process by which state, local, and private sector entities can provide information in a uniform manner. We appreciate the difficult work that has gone into this project and are grateful for the many briefings and meetings that have been provided by the Office of Infrastructure Protection to Members of House Select Committee on Homeland Security. Yet, based on these briefings, and our review of the critical asset lists compiled thus far, we are concerned that methodological flaws in the process are resulting in an incomplete and flawed vulnerability assessment.

According to the briefings we received, the Department has approximately 33,000 critical assets and sites listed in a database. We are told that this database was created from information contributed from state, local, and private sector entities. When questioned about the process by which DHS collects information, representatives admitted that there was not a form or specific guidance given to those providing information so as to ensure that locales across the country provide the same type of information. DHS representatives speaking to us indicated that they rely on a variety of sources for compiling this database, including federal, state, territorial, and local governments and the private sector. It is our understanding that DHS has requested that state homeland security advisors consider coordinating their state's submissions, but that DHS has not provided for an input mechanism that ensures that localities and states around the country give the exact same type of information or even give information at all.

The result of this lack of guidance and outreach is apparent once one looks at the database's contents. Members who looked at the asset list provided for their specific states and communities found that significant government and commercial sites that should have been on the list were not, while sites that no longer existed or represented random businesses were included. Members also discovered that the list was not consistent from town to town and state to state. Without going into specific examples, the database contained assets of a particular nature for one city or state, but did not contain that same type of asset for a similar city or state. We believe this deficiency is a result of DHS' not providing significant guidance to the state and locals on what to include in the information they provide to the Department. We also are concerned that the Department may not have provided guidance as the types of entities and government agencies that should be involved in the local level in providing asset information.

The inconsistencies of critical infrastructure listings between cities suggest that the Department's approach is not comprehensive enough to ensure that all the essential assets of our country are catalogued. The Department cannot start out with flawed instructions to state, local, and private sector entities and then, expect in the end, to have a comprehensive prioritized database. We would urge the Department to consider how to create a more formalized manner in which to receive consistent and useful information from communities throughout the United States.

Indeed, some state and local authorities have confirmed that their input has not been solicited, even though assets from their localities appear in the database. The Department must do a better job in identifying the correct individuals at the state and local level, as well as in the private sector, with whom the Department should be coordinating the vulnerability assessment process. Assistant Secretary Robert Liscouski testified at an April 21 Committee hearing that the completion of the assessment is "outside the control of" the Department and relies heavily on cooperation from state and local governments, as well as the private sector. We agree with this assessment. The effective integration of state and local input, however, is within the control of the Department and it must find a way to better coordinate with state and local officials.

We are concerned that the issues identified with the creation of the 33,000-asset database are resulting in a flawed prioritized asset list. The Department is undertaking an effort to take the larger database and identify a smaller set of assets that are "priority" sites in need of protection. It is our understanding that this prioritized list will include some of our most critical assets, including but not limited to government facilities, financial centers, utilities, and transportation facilities. If, however, the initial database does not contain an important critical asset, the Department cannot include that asset on its prioritized list. For example, if a major telecommunications or Internet backbone company is not in the larger database, the Department's efforts to prioritize the country's telecommunications and cyber infrastructures would be flawed. Likewise, if a significant state government building is missing from the database, the Department's efforts to identify key governmental assets that need to be protected would be lacking. The creation of a formalized and uniform process for receiving information, as well as improving the Department's coordination efforts with state and local authorities, would eliminate this issue.

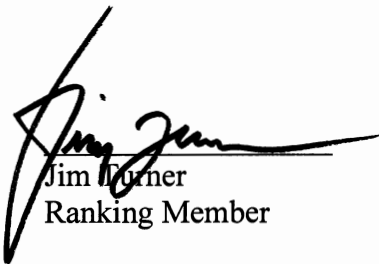
Finally, it is unclear how assets labeled as "soft targets" are integrated into the asset database and, consequently, the Department's protection programs. For example, what initiatives are in place to assist state and local authorities in the protection of educational facilities, including secondary schools and universities? As the Department collects information from state and local authorities, these facilities should be included in the information that the Department gathers.

Likewise, the Department should be working to ensure that state and local authorities understand how to protect these facilities in a comprehensive manner.


We are very interested in making sure that DHS has the resources, including personnel and tools to conduct a comprehensive vulnerability assessment of the nation's critical assets. If current resources are inadequate, Congress needs to know that as soon as possible so that we can take steps to correct the problem.

We hope to continue to work with you and the Department on improving the vulnerability assessment. To further this effort, we request that you provide to the Committee a specific timeline that details the progress the Department has made in completing the risk assessment, when the initial comprehensive risk assessment is expected to be completed, and the significant milestones that are being used to measure the Department's progress.

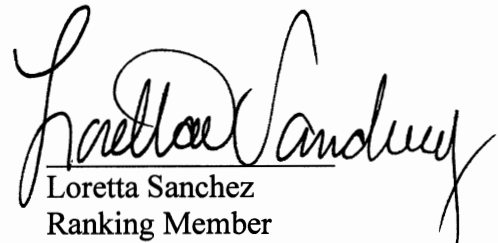
Sincerely,



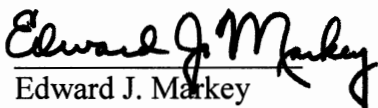
Jim Turner
Ranking Member



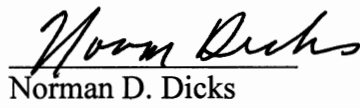
Zoe Lofgren
Ranking Member
Subcommittee on
Cybersecurity, Science,
Research & Development



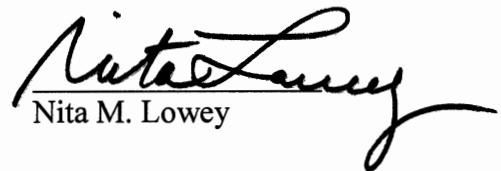
Loretta Sanchez
Ranking Member
Subcommittee on
Infrastructure and
Border Security



Edward J. Markey



Norman D. Dicks



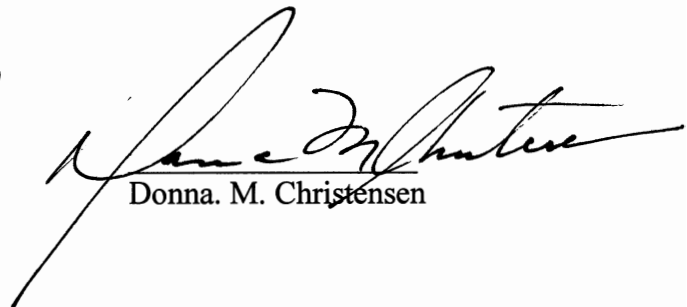
Nita M. Lowey



Robert E. Andrews



Sheila Jackson-Lee



Donna M. Christensen



Bob Etheridge



James R. Langevin



Kendrick B. Meek